AL FRANKEN
MINNESOTA

SUITE
SH-309
202-224-5641

United States Senate

WASHINGTON, DC 20510-2309

June 27, 2012

The Honorable Kathleen Sebelius
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue SW
Washington, D.C. 20201

Dear Secretary Sebelius:

Electronic health records (EHRs) have the potential to reduce medical errors, lower costs, improve treatment, and save lives. To realize that potential, however, patients and providers must have confidence in the privacy and security of sensitive health information that is stored electronically. It is imperative that the Department of Health and Human Services (HHS) use its regulatory authority to safeguard patient data and secure patient trust. I urge you to issue long overdue, statutorily required guidance on the "minimum necessary" standard, which governs the type and amount of protected health information that entities can share. I also ask that you continue take steps to address the security of protected health information (PHI) that is stored on portable media, like laptops.

Guidance on the "Minimum Necessary" Standard. The Health Insurance Portability and Accountability Act (HIPAA) required HHS to issue regulations governing the privacy and security of PHI. The ensuing regulations provided that covered entities may use, disclose, or request only the minimum amount of PHI that is necessary to accomplish the intended purpose of the use, disclosure, or request. However, there emerged confusion as to the meaning of this "minimum necessary" standard. So, in 2009, when Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act, it required HHS to issue guidance on what constitutes 'minimum necessary' PHI under the rules. The HITECH Act required that the guidance be issued by August 17, 2010. That guidance still has not been released, however; it now is nearly two years overdue.

As a result, there appears to be ongoing confusion in the field about legal requirements, and HHS's delay in issuing these guidelines may be contributing to troubling disclosures of sensitive patient information. For example, I recently held a field hearing of the Senate Committee on Health, Education, Labor, and Pensions (HELP), in which I heard about allegations that Accretive Health had mishandled Minnesotans' sensitive PHI. It appears that, for at least some period of time, Accretive Health's off-site debt collectors had unrestricted access to patients' medical records. I also heard testimony about an Accretive Health employee whose laptop contained PHI for hospitals and services unrelated to that employee's job functions – information that the employee simply did not need to perform his job. Nonetheless, Accretive Health's Vice President testified that he believed that his company was in compliance with the rules. Had the "minimum necessary" guidance been released timely, hospitals and the

AL FRANKEN
MINNESOTA

SUITE
SH-309
202-224-5641

United States Senate
WASHINGTON, DC 20510-2309

businesses with which they contract for services may have had the clarification they needed to prevent violations of patient privacy.

Protecting Portable PHI. According to HHS statistics, approximately 1.9 million people have been affected by data breaches involving PHI that was stored on unencrypted portable devices, like laptops. During the recent field hearing that I chaired, I heard testimony about the theft of an unencrypted laptop that contained PHI for more than 23,000 patients and listed the names of an additional 242,000 patients. In November, I chaired a hearing in the Judiciary Subcommittee on Technology, Privacy, and the Law during which I heard from experts about similar cases in which patients' privacy was compromised. Despite these incidents, the 2011 Health Information Management Systems Society (HIMSS) Security Survey indicates that less than half of hospitals and a quarter of medical practices encrypt portable devices.

Encrypting portable devices that contain PHI is considered an industry best practice, but it is not required under existing law. Today I am introducing legislation that will require encryption of portable devices that contain PHI, and I am hopeful that that legislation can move through Congress quickly. But HHS can act immediately to secure patient data. I am encouraged by two proposed HHS efforts to do so: (1) making encryption a criterion for participation in the Nationwide Health Information Network, and (2) requiring participants in the Meaningful Use Incentive program to conduct a security risk analysis that includes encryption practices. However, HHS should also issue guidance on a minimum standard of encryption; furthermore, this guidance must be able to evolve to keep pace with changing technology. And HHS doesn't have to wait for Congress to act, either: with existing authority, it can update the Security Rule to require encryption of portable electronic devices containing PHI.

I respectfully request that you issue a final version of the "minimum necessary" guidance required under the HITECH Act and provide my office with a written statement describing the steps that HHS is taking and will take to secure PHI that is stored on portable devices. Thank you for your consideration of this important issue. I look forward to your response.

Sincerely,

Al Franken
United States Senator